The Software Alliance

BSA

BSA
국제 사이버보안 정책 프레임워크

목차

들어가며

전 세계 각국의 정부는 점점 더 복잡하고 다양한 사이버 보안 위협에 직면하고 있습니다. 매년 사이버 범죄는 세계 경제에서 수천억 달러를 고갈시키고 비즈니스 서비스를 중단시키며 혁신을 저해하고 일자리 증가를 저지합니다. 국가가 후원하는 공격자를 비롯하여 악의적인 해커는 중요 인프라 및 정부 서비스를 위협하고, 광범위한 경제 피해를 입히고, 심하게는 인명 손실을 초래합니다. 안타깝게도 이러한 위험은 더 이상 가상의 것이 아닙니다. 악의적인 사이버 활동으로 인해 전 세계에서 정전, 항구 폐쇄, 금융 거래 중단 및 전국적인 선거 방해가 초래되고 있습니다.

정부가 이러한 위협에 효율적으로 대처할 수 있는 능력은 스마트하고 민첩한 정책을 수립하여 사이버 보안에 대한 균형 잡히고 포괄적인 접근법을 지원하는 데 달려있습니다. 법률과 규칙의 적절한 조합을 채택하고 사이버 보안에 대한 명확한 지침을 수립하는 적절한 기관 및 체계를 구축함으로써 정부는 악의적인 사이버 공격자로부터 방어하고 디지털 경제의 기회를 최대한 활용하며 이해 관계자와의 협력을 강화할 수 있는 견고한 토대를 구축할 수 있습니다. 이러한 조치는 효과적으로 시스템을 보호하며 사이버 공격을 방지 및 완화하고 공격에 대응하는 데 필요한 공동의 노력에 있어 각국 정부부터 민간 부문 담당자에 이르기까지 관련된 모든 당사자에게 도움이 될 것입니다.

그러나 사이버 보안 위협은 비교적 여전히 새롭고 매우 빠르게 진화하고 있기 때문에 정부는 대개 모범 사례 또는 모델 정책에 대한 지침이 거의 없는 상황에서 따라잡으려고 애쓰는 처지에 놓여있습니다. 사이버 보안위협으로부터 방어하기 위한 가장 효과적인 정책 접근법을 고려하는 정부를 지원하기 위해 BSA | The Software Alliance는 정책 입안자가 현재의 사이버 보안 정책을 평가하고 개선을 위한 우선순위 영역을 파악하려고 할 때 이 포괄적인 사이버 보안 정책 프레임워크를 고려할 만한 모델로 제공합니다.

BSA의 국제 사이버 보안 정책 프레임워크는 포괄적인 국가 사이버 보안 정책에 권장되는 모델을 제공합니다. 이 프레임워크의 목적은 기초적인 사이버 보안 법규를 고려하는 정책 입안자들과 기존 정책의 공백 및 부족을 검토하는 사람들 모두를 위한 도구를 제공하는 것입니다. BSA는 강력하고 스마트한 사이버 보안 정책을 인터넷의 안정성과 세계 경제의 활력에 대단히 중요한 요소로 여깁니다. 이러한 이유로 BSA는 이 프레임워크에서 명시한 원칙과 비교하여 전 세계 정부가 제안한 정책을 평가할 것입니다.

프레임워크는 세 부분으로 나뉩니다. 첫 번째, 빠른 참조 요약에서는 모델 프레임워크의 주요 요소를 확인합니다. 두 번째 부분에서는 각 요소를 심층적으로 검토하고 각 영역의 정책 접근법을 세밀하게 규정하기 위한 구체적인 원칙을 제시합니다. 마지막 부분에서 프레임워크는 일반적으로 사용되는 용어 정의를 제시합니다. 그리고 이 문서 전체에 걸쳐 사이버 보안 정책을 구현하는 모범 사례의 국제적인 예를 강조합니다.

사이버 보안 위협이 점점 더 정교해지고 위험해짐에 따라 사이버 위협 대응에 대한 국가의 정책 접근법이 불충분하거나 제대로 보정되지 않은 경우 위험이 재앙적 수준까지 커지는 사례가 점점 더 늘어나고 있습니다. BSA는 전 세계 각국의 정부와 협력함으로써 인터넷을 사용하는 전 세계 수십억 명의 시민들을 위해 점점 더 서로 연결되는 인터넷 에코시스템의 보안 및 복원력을 증대하기를 기대하고 있습니다. 사이버 보안 위협 환경이 진화함에 따라 BSA는 끊임없이 세계 정부들의 진행 상황을 평가하여 이 프레임워크를 조정함으로써 정책 입안자들이 보조를 맞출 수 있도록 지원할 것입니다.

섹션 I.
실무 요약

BSA는 매우 중요한 다음 6가지 원칙에 따라 정책 입안자가 모든 사이버 보안 정책을 수립하도록 권장합니다.

1. **정책은 국제적으로 인정받은 기술 표준에 부합해야 합니다.** 국제적으로 인정받은 기술 표준은 사이버 보안에 대한 효과적인 접근법을 정의 및 구현하기 위해 광범위하게 점검된 합의 기반의 프레임워크를 제공하고 공통의 당면 과제에 대한 공통 접근법을 촉진함으로써 협업 및 상호 운용성을 지원합니다.

2. **정책은 위험 기반, 결과 중심 및 기술 중립적인 특성을 띠어야 합니다.** 악의적인 사이버 보안 활동은 시스템마다 다른 위험을 초래합니다. 일반적으로 동일한 유형의 사이버 공격으로부터 방어하는 데에는 여러 접근법이 있습니다. 그리고 전반적으로 시스템 보안 및 복원력을 개선하는 데에도 여러 접근법이 있습니다. 정책은 이러한 변수를 반영하여 서로 다른 수준의 위험을 처리하고 네트워크 및 시스템의 소유자와 운영자가 원하는 보안 수준에 가장 부합한다고 생각하는 기술 및 접근법으로 해당 인프라를 방어할 수 있도록 접근법의 우선순위를 정해야 합니다.

3. **정책은 가능한 경우 시장 중심 메커니즘을 사용해야 합니다.** 정보 기술은 끊임없이 발전하고 있으며, 사이버 보안 위협도 함께 진화하고 있습니다. 기술이나 위협은 국경의 제한을 받지 않습니다. 즉, 정부 구조나 규제 집행에 과도하게 의존하면 원하는 결과를 달성하지 못할 가능성이 있습니다. 시장의 힘을 활용하여 사이버 보안을 촉진하는 정책은 변화하는 보안 환경과 보조를 맞추고 가장 광범위한 효과를 달성하는 데 가장 성공적일 것입니다.

4. 정책은 혁신을 장려하기 위해 유연하고 상황에 맞춰 조정할 수 있어야 합니다 정보 기술 및 수백만 개의 일자리 기술 지원은 새로운 솔루션을 혁신할 수 있는 역량에 달려있습니다. 변화하는 위협에 뒤처지지 않으려면 사이버 보안을 끊임없는 혁신해야 합니다. 정책은 유연하고 상황에 맞춰 조정할 수 있어야 합니다. 이를 통해 기업이 새로운 당면 과제에 대한 새로운 접근법을 개발할 수 있으며, 해당 기업의 솔루션을 이용하는 고객들에게 혁신적인 제품을 제공할 수 있습니다.

5. 정책은 공공 부문과 민간 부문의 협업에 뿌리내려야 합니다 사이버 보안은 정부 및 민간의 이해 관계자 전체의 공동 책임입니다. 대개 정부가 중요한 사이버 보안 도구 및 정보를 보유하고 있지만, 민간 부문도 악의적인 사이버 활동의 표적이 되는 중요 인프라 및 기술 플랫폼의 중요한 요소를 관리할 뿐만 아니라, 그러한 위협으로부터 방어하는 데 필요한 많은 사이버 보안 도구 및 서비스도 책임지고 있습니다. 정부는 민간 부문과의 긴밀한 협업을 통해서만 진정으로 사이버 보안 위협과 맞서 싸우면서 디지털 경제의 활력을 지속할 수 있습니다.

BSA의 사이버 보안 정책에 대한 기본 원칙

사이버 보안 정책은 다음과 같은 접근법을 채택해야 합니다.

1. **국제적으로 인정받은 표준**에 맞춰 조정
2. **위험 기반, 결과 중심 및 기술 중립적**
3. 가능한 경우 **시장 중심**
4. 혁신을 장려하기 위해 **유연하며 상황에 맞춰 조정 가능**
5. **공공 부문과 민간 부문의 협업**에 뿌리내려야 함
6. **개인정보** 보호 지향

6 정책은 개인정보보호를 지향해야 합니다 사이버 보안에 대한 어떠한 접근법도 악의적인 사이버 활동으로부터 방어하려고 하는 데이터의 무결성을 침해해서는 안 됩니다. 사이버 보안 정책은 개인정보보호 고려 사항에 맞춰 면밀하게 조율되어야 합니다. 주요 고려 사항에는 민간 리더십 보장, 강력한 데이터 보호책 장려, 정보 공유 메커니즘에서 개인 정보 보호 장치, 개인정보보호 강화 기술의 사용을 저해하는 정책 방지가 포함됩니다.

근본적으로 이러한 원칙을 기반으로 하는 BSA의 국제 사이버 보안 정책 프레임워크는 입법 및 행정 조치를 안내하는 세부 원칙을 비롯하여 사이버 보안 정책의 포괄적인 토대를 개략적으로 설명합니다. 다음 차트에 강력한 국가 사이버 보안 정책의 주요 요소가 요약되어 있습니다.

국가 사이버 보안 정책의 주요 요소

정부 조직 및 전략		
체계	✓	사이버 보안을 담당하는 단일 국가 단체를 설립해야 합니다.
	✓	이해 관계자의 역할 및 책임을 명확하게 정의해야 합니다.
	✓	기능적이며 적시에 이루어지는 기관 간 프로세스를 수립해야 합니다.
전략 및 계획	✓	국가 사이버 보안 전략을 발표해야 합니다.
	✓	중요 인프라 사이버 보안 전략을 발표해야 합니다.
	✓	중요 인프라에 대한 최신 국가 사이버 보안 사고 대응 계획을 유지 관리해야 합니다. 부문별 계획을 적절하게 수립해야 합니다.
	✓	Craft Sector-Specific Plans as Appropriate
이해 관계자 참여	✓	공공 부문과 민간 부문의 파트너십 촉진을 위한 체계를 확립해야 합니다.
	✓	하위 국가 및 지방 정부를 지원하기 위한 메커니즘을 만들어야 합니다.
사이버 보안 및 정부		
대비 및 대응	✓	국가 컴퓨터 비상 대응 팀을 편성하고 리소스를 제공해야 합니다.
	✓	위협 정보 공유를 적시에 허가하고 장려해야 합니다.
	✓	사고 보고를 위한 체계를 보정해야 합니다.
	✓	개인 데이터 침해 통지를 위한 일관되고 합리적인 표준을 확립해야 합니다.
	✓	정부는 취약성 처리 및 공개에 대한 투명하고 조정된 프로세스를 수립해야 합니다.
정부 조달	✓	인수를 기술 중립적으로 유지해야 합니다.
	✓	라이선스가 부여된 소프트웨어를 사용해야 합니다.
	✓	소프트웨어가 벤더의 지원을 받는지 확인해야 합니다.
	✓	클라우드 서비스의 보안 이점을 활용해야 합니다.
	✓	인수 프로세스에 보안 고려 사항을 부가해야 합니다.
	✓	IT 시스템을 스마트하고 안전하게 관리해야 합니다.
	✗	국내 제품/서비스 선호 요구 사항을 피해야 합니다.
연구 및 개발	✓	사이버 보안 기술 및 도구에 대한 연구 및 개발을 지원해야 합니다.
사이버 보안 및 민간 부문		
중요 인프라	✓	보안 성과에 집중해야 합니다.
	✓	위험 기반의 유연한 정책 프레임워크를 사용해야 합니다.
	✗	중요(정보) 인프라에 대한 너무 폭넓은 정의를 피해야 합니다.
	✓	국제적으로 인정받은 표준에 맞춰 중요 인프라 보안을 조정해야 합니다.
	✗	지역의 고유한 보안 표준을 피해야 합니다.
	✓	인증 제도는 균형적이고 투명하며 국제적 기준을 따라야 합니다.
	✗	소스 코드 및 기타 지적 재산의 공개 요구를 거부해야 합니다.

국가 사이버 보안 정책의 주요 요소

사이버 보안 및 민간 부문(계속)		
소비자 제품	✔	시장 중심 솔루션을 촉진해야 합니다.
	✔	국제적으로 인정받은 표준의 채택을 장려해야 합니다.
데이터 흐름	✔	비즈니스 목적의 국가 간 데이터 흐름을 지원해야 합니다.
	✘	데이터 현지화 요구 사항을 피해야 합니다.
	✔	신기술을 사용할 수 있도록 지원하는 정책 환경을 유지해야 합니다.
사이버 보안 및 시민		
인식	✔	공공의 사이버 보안 인식에 투자해야 합니다.
	✔	소비자 선택에 영향을 미치는 도구를 만들어야 합니다.
인력 개발	✔	모든 수준의 교육에서 사이버 보안 인식을 증진해야 합니다.
	✔	사이버 보안 교육 및 훈련에서 다양성의 우선순위를 정해야 합니다.
	✔	사이버 보안 취업을 위한 대체 경로를 지원해야 합니다.
형사 법규		
사이버 범죄	✔	사이버 범죄에 대한 부다페스트 협약과 일관된 포괄적인 법적 프레임워크를 확립해야 합니다.
	✔	범죄 의도가 있는 공격자에게만 형사 책임을 적용해야 합니다.
	✔	법 집행을 위한 기술 교육 및 지원을 제공해야 합니다.
국제 협정		
국제 사이버 보안 협력 촉진	✔	외교 정책에 사이버 보안 협력을 통합해야 합니다.
	✔	국제 협력 활동에 참여해야 합니다.
	✘	수출 통제 정책이 합법적인 사이버 보안 활동을 저해하지 않도록 해야 합니다.
국제 의무 지지	✔	해당 영역이 국제 사이버 공격에 사용되지 않도록 해야 합니다.
	✔	인터넷에서 개인정보 및 인권을 보호해야 합니다.
	✘	IT 시스템 제조업체가 국가 후원 해킹을 지원하게 만드는 명령을 피해야 합니다.

섹션 II.
심층 검토

정부 조직 및 전략

모범사례

국제 네트워크 및 정보 보안 조정을 위한 NCA(국가 주무 당국)

효과적인 협업은 다양한 이해 관계자 전체에 걸쳐 명확하고 열린 소통 유지와 민첩한 조정에 달려 있습니다. 이러한 협업을 촉진하기 위한 모범 사례는 EU의 2016 네트워크 및 정보 보안 지침(Network and Information Security Directive)에 명시된 대로 네트워크 및 정보 보안을 위한 NCA(국가 주무 당국)를 파악하는 것입니다. NCA는 초국가적인 사이버 보안 위협에 대한 국가 간 협력을 지지하며 다른 정부와 연락하고 국가 이해 관계자 전체에 걸쳐 중요한 사이버 보안 정보의 공유를 촉진하기 위해 "단일 연락 지점" 역할을 합니다. 사이버 보안에 대해 주요 책임을 맡은 단일 국가 조직이 대개 NCA 역할을 합니다.

체계

사이버 보안을 담당하는 단일 국가 단체를 설립해야 합니다. 사이버 보안과 관련된 주요 정책 및 활동에 대한 책임이 여러 정부 기관에 분산되어 있을 수 있습니다. 그러나 정부의 사이버 보안에 대해 가장 중요한 책임을 지는 단일 정부 단체를 정해두면 정부가 사이버 보안 위협 및 과제에 대비하고 대응할 때 명확성, 일관성 및 조정을 보장할 수 있습니다. 정부는 사이버 보안에 대해 가장 중요한 책임을 지는 단일 조직을 정하고 다른 정부 기관의 사이버 보안 활동을 지휘 및 감독할 권한을 해당 조직에 부여해야 합니다. 일반적으로 국내 및 국제적 경제 이익에 대한 광범위한 파급 효과 때문에 민간 법인(섹션 III, 정의 참조)이 전반적인 사이버 보안 활동을 주도해야 합니다.

이해 관계자의 역할 및 책임을 명확하게 정의해야 합니다. 각 국가는 체계가 서로 다르고 통치 구조도 다르므로 사이버 보안 책임이 사실상 매우 다양한 방식으로 배정 및 분배될 수 있습니다. 일부 국가는 사이버 보안 정책 활동을 몇몇 한정된 그룹의 정부 기관으로만 제한하는 중앙 집중식 모델을 선호하는 반면, 다른 국가는 책임을 정부 전체에 걸쳐 광범위하게 분산시킨 모델을 선호합니다. 어떤 모델을 선택하든, 정부 내각, 정부 기관, 산업 이해 관계자 및 비정부 조직을 비롯한 모든 관련 이해당사자의 역할 및 책임을 명확하게(혼동이나 중복을 피할 수 있는 방식으로) 정의하고 배정하는 것이 중요합니다.

기능적이며 적시에 이루어지는 기관 간 프로세스를 수립해야 합니다. 사이버 보안을 위한 정부의 조직 체계와 관계없이 사이버 보안 정책은 민간 기관과 군사 기관 모두를 비롯하여 여러 정부 기관의 활동 및 목표에 영향을 줍니다. 기능적 기관 간 프로세스는 이러한 기관 간 이해관계의 균형을 유지하고 분쟁이 발생할 경우 해당 분쟁에 대한 판정을 내리는 데 필수적인 역할을 합니다. 또한 기관 간 구조에서는 결의를 통해 시간에 민감한 결정을 적시에 도출하는 프로세스를 수립해야 합니다.

전략 및 계획

국가 사이버 보안 전략을 발표해야 합니다. 국가 사이버 보안 전략은 사이버 보안에 대한 국가의 전반적인 접근법을 제시하며, 국가 차원의 전략 및 정책 일관성을 보장하는 데 중요한 문서입니다. 효과적인 국가 사이버 보안 전략은 국가가 직면한 사이버 보안 위협을 개략적으로 설명하고, 목표를 파악하여 우선순위를 정하고, 주요 정부 및 산업 이해 관계자 사이의 역할 및 책임을 설명하고, 구현을 위한 기간 및 메트릭을 설정합니다. 그뿐만 아니라 국제 사이버 보안 활동과 사이버 보안 활동에 영향을 미치는 기타 국가적 활동 모두의 맥락에서 국가 사이버 보안 활동의 입지를 정합니다. 국가 전략은 정부 이니셔티브를 주도할 뿐만 아니라 의사 결정자들 간의 주요 쟁점에 대한 인식을 제고하고 정부 정책 및 활동을 대중에게 알리는 데에도 중요합니다. 이러한 전략은 정부 기관, 업계, 학계 및 시민 단체를 비롯하여 모든 관련 이해당사자 대표와의 협의를 통해 협조적으로 개발해야 합니다. 국가 전략은 국가 차원에서, 이상적으로는 정부 수반이 발표해야 하며 국가적 맥락 내에서 커뮤니티 기반 모범 사례뿐만 아니라 중앙 정부, 하위 국가 정부 및 지방 정부의 접근법을 통합해야 합니다. 마지막으로, 국가 전략에 구체적인 과제, 마감일 및 메트릭을 포함하여 해당 전략을 실질적으로 실행해야 합니다.

중요 인프라 사이버 보안 전략을 발표해야 합니다. 또한 정부는 보호가 가장 필요한 중요 서비스와 인프라(섹션 III, 정의 참조) 간에 분명한 우선순위를 평가 및 설정해야 합니다. 예를 들어 전기 배전망, 급수 시스템 및 교통 시스템은 기본적인 인간의 욕구를 충족시키는 데 기여하며 일반적으로 국가의 중요 인프라 전략에 따라 우선적으로 보호되어야 합니다. 그러나 각 부문 내에서 모든 자산, 시스템, 네트워크, 데이터 및 서비스가 동일하게 필수적인 것은 아닙니다. 따라서 전략은 도를 넘지 않으며 필요하지 않은 곳에 준수 부담을 부과하지 않는 것이 중요합니다. 실질적으로 중요한 시스템과 동일한 방식으로 중요하지 않은 시스템을 취급하면 혁신 속도와 성장 속도를 불필요하게 저하시킬 뿐만 아니라 제한된 보안 리소스를 잘못 할당할 위험도 발생합니다. 따라서 의사 결정자가 객관적인 기준 및 관련 이해당사자의 의견에 따라 국가 인프라를 평가하고 중요 서비스 및 기능을 제공하는 국가 인프라를 판단하는 것이 중요합니다. 중요한 사이버 보안 사고(섹션 III, 정의 참조)로 인한 해당 인프라의 침해, 손상 또는 파괴는 결과적으로 대중에게 상당한 피해를 줄 수 있습니다. 정부가 보호를 위해 중요 인프라를 평가하고 우선순위를 정함에 따라 그 결과를 중요 인프라 보호 계획에 반영해야 합니다. 이러한 계획에서는 우선순위가 높은 중요 인프라를 파악하고, 중요 인프라 커뮤니티의 정부 및 민간 부문 참가자가 협력하여 위험을 관리하고보안 및 복원력 성과를 달성하는 방식을 개략적으로 설명합니다.

중요 인프라에 대한 최신 국가 사이버 보안 사고 대응 계획을 유지 관리해야 합니다. 중요 인프라 보호 계획은 국가의 중요 인프라 커뮤니티 내 정부 기관 및 기타 이해 관계자가 어떻게 위험을 관리하고 위협으로부터 방어할 것인지 정의하며, 국가 사고 대응 계획은 이러한 이해 관계자가 중요한 사이버 보안 사고(섹션 III, 정의 참조)에 어떻게 대응할 것인지를 정의합니다. 국제적 모범 사례에 따르면 이러한 계획에서는 국가가 중요 인프라에 영향을 주는 중요한 사이버 보안 사고에 대응하고 그로부터 복구하는 방법을 지원하는 역할, 책임, 역량 및 조정 체계를 분명히 설명해야 합니다. 국가 사고 대응 계획은 중요 인프라에 영향을 주는 중요한 사이버 보안 사고가 발생했을 때 대응 및 복구에 대한 정부 전체, 국가 전체 및 국제적으로 조율된 통일된 접근법을 사용하기 위해 활용할 수 있는 지침을 제공합니다. 그리고 국가, 부문 및 개별 조직의 사이버 운영 계획을 위한 공통 원칙 및 전략적 프레임워크를 분명히 설명합니다.

모범사례

다중 이해 관계자 소집 프로세스

정부는 특정 당면 과제 또는 위협에 중점을 두며 가장 관련 있는 공공 및 민간 부문 이해 관계자의 역량을 극대화하는 대상 실무 그룹을 소집함으로써 중요한 역할을 할 수 있습니다. 민간 산업계의 이해 관계자들은 대개 현재의 두드러진 사이버 보안 위협에 대처하기 위해 기꺼이 협업하지만, 정부가 관련 이해 관계자를 파악 및 소집할 수 있으며 당면 과제 및 위협에 대한 인텔리전스 중심의 이해와 소집 권한을 모두 활용할 때 이러한 협력은 가속화될 수 있습니다. 다중 이해 관계자 프로세스는 정부 및 민간 부문 역할의 모든 관련 이해당사자가 제시하는 의견을 정책 또는 운영 이니셔티브의 형성 과정에서 수렴하고 이해 관계자가 성과에 집중하도록 합니다.

부문별 계획을 적절하게 수립해야 합니다. 사이버 보안 보호의 특정 요소가 모든 영역에 걸쳐 적용되고 국가 및 국제 조직에서 많은 권장 사항을 사용할 수 있지만, 특정 법인의 비즈니스 요구에 맞게 조정된 지침이나 특정 부문의 고유한 위험 또는 특정 활동을 처리하는 방법을 제공하는 지침도 필요합니다.

이해 관계자 참여

공공 부문과 민간 부문의 파트너십 촉진을 위한 체계를 확립해야 합니다. 효과적인 사이버 보안을 구현하려면 모든 이해 관계자 간의 협업 및 조정이 필요합니다. 공공 부문과 민간 부문 간의 진정한 파트너십은 비정부 법인이 대개 교통, 건강, 금융, 에너지 및 기타 필수적인 부문을 제어하는 인프라를 비롯하여 많은 중요 인프라를 관리하고 운영하기 때문에 특히 중요합니다. 정부는 공공 부문과 민간 부문의 자발적인 파트너십을 촉진하기 위한 법률 및 체계를 확립해야 합니다. 이 러한 법률 및 체계는 최소한 (1) 위협 및 취약성 정보의 자발적 공유를 위한 체계, 법적 권한 및 보호, (2) 사이버 보안 위협을 중단시키기 위해 공공 부문과 민간 부문이 자발적으로 노력하는 운영 협업을 위한 법적 권한, (3) 인식 및 홍보 활동을 위한 메커니즘 그리고 (4) 부문 내에서의 공공과 민간 협업을 다루어야 합니다. 하위 국가 및 지방 정부를 지원하기 위한 메커니즘을 만들어야 합니다. 하위 국가 및 지방 수준의 정부 기능은 대개 시민 및 기업의 일상적인 생활과 활동을 지원하는데국가 차원의 정부 기능만큼 중요하거나 그보다 훨씬 더 중요할 수 있지만, 하위 국가 및 지방 정부가 일반적으로 이러한 기능에 지장을 줄 수 있는 사이버 공격으로부터 방어하는 데 국가 정부와 동일한 수준의 역량을 유지할 수는 없습니다. 하위 국가 및 지방 정부는 그 자체로 중요 인프라이며, 국가 정책은 하위 국가 및 지방 정부에 기술 및/또는 재무 지원을 제공하여 자체적으로 강력한 사이버 방어 체제를 개발하도록 하는 등 해당 인프라를 방어하기 위한 메커니즘을 확립해야 합니다.

사이버 보안 및 정부

대비 및 대응

국가 컴퓨터 비상 대응 팀을 편성하고 리소스를 제공해야 합니다. 국가적으로 중요한 정보 네트워크 및 시스템의 기밀성, 무결성 또는 가용성을 위협하거나 시민 개개인에게 광범위한 위험을 초래하는 가장 위급하고 중요한 사건을 관리할 수 있는 사고 대응 역량을 확립해야 합니다. 국가 및 하위 국가 또는 지방 수준의 CERT(컴퓨터 비상 대응 팀)는 물론, CSIRT(컴퓨터 보안 사고 대응 팀)는 사이버 복원력 향상에 중대한 역할을 할 수 있습니다. 이러한 법인은 (1) 공격 피해자에게 사고 대응 서비스를 제공하고, (2) 정부 및 민간 부문의 주요 이해 관계자 및 경우에 따라서는 광범위한 대중과 취약성 및 위협에 관한 정보를 공유하고, (3) 컴퓨터 및 네트워크 보안을 향상시키는 데 도움이 되는 기타 방법을

제공할 수 있습니다. 국가 정부는 국가 차원에서 컴퓨터 비상 대응 팀을 합법적으로 편성하고, 중요한 사이버 보안 사고 및 기타 대규모 국가 사이버 사건에 대비하고 이를 유능하게 처리할 수 있도록 해당 팀에 충분한 리소스를 제공해야 합니다.

위협 정보 공유를 적시에 허가하고 장려해야 합니다. 영향받는 당사자는 물론, 공격으로부터 방어하기 위한 수단을 개발할 수 있는 역량을 보유한 법인과 사이버 보안 위협, 취약성 및 사고에 대한 정보를 공유할 수 있는 능력이 필수적입니다. 공격은 민간 부문과 정부 담당자 모두를 표적으로 삼고 국경을 넘나들기 때문에 정보 공유 정책에서는 정부와 민간 부문 간에, 민간 부문의 법인 간에 그리고 정부 법인 간에 공유를 촉진해야 합니다. 이 목적을 달성하기 위해서 다음 6가지 원칙에 따라 효과적인 사이버 보안 정보 공유 법률 또는 정책을 제정해야 합니다.

1. **법적 책임 면제.** 정책은 잠재적인 법적 책임 또는 규제 결과를 명시적으로 제한함으로써 민간 법인이 사이버 보안 위협 지표(섹션 III, 정의 참조)에 대한 정보를 국내 및 국제적으로 다른 민간 법인 또는 정부와 자발적으로 공유할 수 있도록 해야 합니다. 이러한 제한은 이 정보를 공유하고 수신하는 데 모두 적용되어야 합니다. 또한 정책은 이러한 접근법의 자발성 격려라는 기본 취지에 부합되게 기업이 다른 민간 법인 또는 정부와 정보를 공유하지 않기로 선택한 경우에도 법적 책임을 지지 않도록 해야 합니다.

2. **개인정보보호.** 정책은 공유된 사이버 보안 위협 정보에 영향을 받는 사람들의 개인정보를 보호해야 하며, 사이버 보안 위협 지표를 적시에 공유하는 능력을 저해하지 않아야 합니다.

3. **다방향 공유.** 정책은 민간 법인이 정부 및 민간 부문 당사자 모두와 그리고 정부부터 민간 부문 당사자에 이르기까지 정보를 공유하도록 촉진하는 동시에 적절한 거래 협정 및 부문별 협정을 체결할 수 있는 유연성을 영향받은 당사자에게 제공해야 합니다.

4. **적시성.** 정책은 정부 담당자가 적절한 사이버 보안 위협 정보를 민간 부문 당사자와 공유하도록 허가 및 권장하고, 자동화된 메커니즘을 비롯하여 다양한 방법을 통해 해당 정보를 공유하는 데 소요되는 시간을 단축해야 합니다.

5. **민간 주도.** 정책은 민간 부문과 정부 간에 정보를 공유할 수 있는 민간 포털을 구축해야 합니다.

6. 사이버 보안 용도. 정책은 수신자가 공유된 사이버 보안 위협 정보를 다른 목적으로는 사용하지 않고 사이버 보안 증진 용도로만 사용하도록 해야 하며, 정보를 정부와 공유할 경우 해당 정보를 사이버 보안 증진 용도로만 사용하거나 한정된 법 집행 활동에만 사용하도록 해야 합니다.

사고 보고를 위한 체계를 보정해야 합니다. 일부 정부는 정부 또는 규제 법인에 중요한 사이버 보안 사고(섹션 III, 정의 참조)를 자발적으로 보고하도록 장려하거나 의무적으로 보고하도록 요구하는 조치를 채택함으로써 사이버 보안 위협 환경에 대한 상황 인식 및 대응을 개선하려고 노력해왔습니다. 자발적인 사고 보고 제도는 정부와 업계 간의 신뢰를 강화하고 보다 강력한 양방향 정보 공유를 촉진할 수 있습니다. 그러한 제도가 의무적이든 자발적이든 상관없이 위험 기반 방식으로 대상을 지정하는 것이 중요합니다. 보고 임계값이 너무 폭넓은 프레임워크는 기업에서 해당 시스템에 발생한 사고를 과도하게 통지하여 알림 피로, 비용 증가 및 운영 방해를 유발하거나 가장 중요한 사고를 파악 및 처리하는 데 어려움을 초래함으로써 의도치 않게 사이버 보안을 저해할 수 있습니다. 대신, 사이버 사고 보고를 위한 메커니즘을 구축하려고 모색하는 정부는 다음과 같은 원칙을 채택해야 합니다.

» **명확한 보고 체계 확립.** 수많은 정부 및 규제 기관이 특정 사고에 관여할 수 있다는 점을 고려해 볼 때 국가 컴퓨터 비상 대응 팀을 통해 이상적으로 조율된, 효율적이고 이용하기 쉬운 보고 체계를 시행해야 합니다. 이 체계는 데이터의 안전하고 민첩한 전송 및 사용을 보장하는 기술적 역량을 통해 지원되어야 합니다.

» **위험에 따라 보고 임계값 보정.** 모든 사이버 사고가 중요한 것은 아닙니다. 그리고 보고가 지나치게 많으면 보고를 받는 쪽의 법인이 감당할 수 없게 되어 중대한 위협에 대한 즉각적인 대응력이 떨어질 수 있습니다. 대신, 보고는 (1) 국가에 가장 긴요한 중요 인프라 부문, (2) 영향받은 시스템의 기밀성, 가용성 또는 무결성에 상당한 영향을 미치는 사고 및 (3) 사고와 관련된 유용한 정보로 제한되어야 합니다.

» **중복 요구 사항 방지.** 사고 보고 정책은 보고 법인이 여러 규제 제도를 책임을 지는 경우라도 보고 요구 사항의 중복을 방지하기 위해 역할 및 책임(정부 담당자와 보고 법인 모두의 역할 및 책임 포함)을 정의해야 합니다. 정부는 개별 정부 기관 간의 중복 요구 사항을 방지해야 하며, 실질적이고 효율적인 대응을 촉진하기 위해 중요한 사고에 대한 정보 공유 프로세스를 간소화하려고 노력해야 합니다.

» **일관성 유지.** 다양한 산업 또는 상이한 상황에 대한 서로 다른 보고 요구 사항은 혼란을 일으키고 과도한 규제 부담을 유발합니다. 대신, 사고 보고 프레임워크는 국제적으로 인정받은 표준과 널리 용인되는 기타 접근법에 따라 비즈니스 환경에서 유연하고 실용적이어야 하며 부문 전체에 걸쳐 일관성을 유지해야 합니다.

» **자율적이고 합리적인 타임라인.** 타임라인을 인위적으로 짧게 설정하면 불완전하거나 부정확한 보고가 생성되며, 대개 영향받는 법인이 사고에 대해 전체 그림을 그리거나 진단하기 전에 미비한 정보를 보고하게 됩니다. 사고 보고 프레임워크는 보고의 무결성을 침해하거나 특정한 마감일을 지정하지 않고 합리적인 기간 내에 사고가 보고될 것이라는 기대를 할 수 있어야 합니다.

개인 데이터 침해 통지를 위한 일관되고 합리적인 표준을 확립해야 합니다. 모든 비즈니스 및 조직에 적용할 수 있는 개인 데이터 침해 통지 시스템을 구축하면 개인 데이터에 대한 강력한 보호를 보장하도록 법인에 유인가를 제공할 수 있는 동시에 데이터 주체는 해당 데이터가 침해된 경우 자신을 보호하는 조치를 취할 수 있습니다. 그러나 이러한 시스템은 중요하지 않은 통지의 발급을 방지하도록 신중하고 세밀하게 구축해야 합니다. 사용자에게 해를 끼칠 심각한 위험이 있는 경우에만 통지해야 합니다. 침해 당시에 효과적인 업계 관행 또는 산업 표준으로 널리 용인되고 있는 관행 또는 방법을 통해 허가받지 않은 제3 자가 문제의 손실된 데이터를 사용하거나 읽거나 이해할 수 없게 된 경우에는 통지가 필요하지 않습니다. 침해 통지가 필요한 경우 침해의 특성 및 범위를 평가하는 데 필요한 시간 및 침해로 인해 데이터 주체에 중대한 해를 끼칠 가능성이 있는지 여부를 고려하여 합리적인 기간 내에 통지해야 합니다. 타임라인을 인위적으로 짧게 설정하면 보고의 완전성 및 정확성이 훼손되고 사고 대응에 지장을 줄 수 있습니다. 대신, 통지 표준은 보고의 무결성을 침해하거나 특정한 마감일을 지정하지 않고 합리적인 기간 내에 사고가 보고될 것이라는 기대를 할 수 있어야 합니다.

정부는 취약성 처리 및 공개에 대한 투명하고 조정된 프로세스를 수립해야 합니다. 정부는 제품 및 서비스 취약성을 처리할 수 있는 명확한 원칙 기반의 정책을 수립해야 합니다. 이 정책은 CVD(Coordinated Vulnerability Disclosure) 원칙[1] 에 따라 제품 및 서비스 취약성을 누적, 구매, 판매 또는 활용하는 대신, 벤더에 보고하라는 강력한 지시를 반영해야 합니다. CVD 프로그램은 취약성이 공개되기 전에 벤더가 해당 취약성을 수정함으로써 피해 가능성을 줄이고, 보안 연구 및 취약성 공개에 대한 책임감 있는 접근법을 장려하며, 정부와 기술 벤더 모두가 예상치 못한 일을 피할 수 있도록 지원합니다. 그리고 정책은 대중에게 투명해야 합니다.

1 예를 들어 http://standards.iso.org/ittf/PubliclyAvailableStandards/c045170_ISO_IEC_29147_2014.zip에서 제공하는 ISO/IEC 29147(취약성 공개) 또는 https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf에 나와 있는 CVD(Coordinated Vulnerability Disclosure)에 대한 CERT 가이드를 참조하십시오.

정부는 제품 및 서비스 취약성을 처리할 수 있는 명확한 원칙 기반의 정책을 수립해야 합니다 이 정책은 CVD(Coordinated Vulnerability Disclosure) 원칙에 따라 제품 및 서비스 취약성을 누적, 구매, 판매 또는 활용하는 대신, 벤더에 보고하라는 강력한 지시를 반영해야 합니다

정부 조달

인수를 기술 중립적으로 유지해야 합니다. 효과적인 사이버 보안에는 방어 네트워크에 대한 계층적이며 다면적인 접근법이 포함됩니다. 흔히 말하는 혁신적인 사이버 보안 솔루션은 공통 목표를 달성하는 데 많은 기술적 접근법을 활용할 수 있습니다. 정부 기관이 가장 혁신적이고 효과적인 사이버 보안 솔루션을 확보할 수 있도록 인수 규칙 및 규정은 기술 중립적이어야 합니다. 조달 정책은 보안 목표를 명시해야 합니다. 그러나 해당 목표를 달성하는 최상의 방법에 대한 기술적 접근법은 벤더가 결정하게 해야 합니다.

라이선스가 부여된 소프트웨어를 사용해야 합니다. 라이선스가 부여되지 않은 소프트웨어를 사용하면 기업 및 정부 기관의 맬웨어 감염 및 기타 보안 취약성 위험이 커집니다. 실제로 글로벌 리서치 회사인 IDC의 2015년 연구에 따르면 라이선스가 없는 소프트웨어의 존재와 맬웨어 발생률 간에 강력한 상관관계가 있음이 확인되었습니다.[2] 라이선스가 없는 소프트웨어는 맬웨어 노출과 관련된 위험을 완화시킬 수 있는 중요한 보안 업데이트를 받을 가능성이 작기 때문에 이러한 소프트웨어를 사용하면 유해한 사이버 보안 사고의 위험이 커집니다. 또한 신뢰할 수 없는 소스로부터 나온 라이선스가 없는 기술에는 악의적인 공격자가 삽입한 임베디드 맬웨어가 포함되어 있을 수 있습니다. 안타깝게도 적절한 라이선스가 없는 소프트웨어의 사용 (정부 기관 및 계약업체에 의한 사용 포함)은 여전히 전 세계적으로 중요한 문제입니다. 많은 경우에 정부에서 라이선스가 없는 소프트웨어를 사용하는 것은 단순히 해당 정부 부처에서 해당 시스템에 상주하는 소프트웨어 자산이 미치는 영향을 제대로 인식하지 못하기 때문일 수 있습니다. 대부분의 기관에는 소프트웨어 라이선스를 관리할 수 있는 적절한 정책이 없습니다. 투명하고 검증 가능한 SAM(소프트웨어 자산 관리) 방침은 법인에서 라이선스가 없는 소프트웨어를 사용하는 상황은 물론, 보유한 라이선스가 사용자 수를 훨씬 초과하는 상황을 파악합니다. 과소 라이선싱은 법적 책임 및 보안 위험을 야기하며, 과다 라이선싱은 비효율성과 불필요한 비용을 초래합니다. 정부 기관은 국제적으로 인정받은 표준에 따라 고유한 조달 및 소프트웨어 자산 관리에 대한 SAM 방침을 채택해야 하며 이를 통해 적절한 라이선스가 있는 소프트웨어만 사용함으로써 사이버 보안을 강화하고 비용을 절감해야 합니다. 또한 정부 기관은 소프트웨어 구성 요소 사무소와 지원 계약업체에도 강력한 소프트웨어 자산 관리 방침을 채택하도록 요구해야 합니다.

소프트웨어가 벤더의 지원을 받는지 확인해야 합니다. 정부 기관이 점점 더 IT 리소스를 제품보다는 온라인 서비스로 구매 및 "소비"함에 따라 정부 기관은 자사의 서비스에 대해 강력하고 안정적인 지원을 제공하는 것으로 입증된 실적을 보유한 IT 공급업체와 협력하는 것이 그 어느 때보다 더 중요해졌습니다. 따라서 정부 정책은 공급업체(또는 다른 상업적 파트너)가 안정적인 지원을 제공하는 IT 솔루션을 우선적으로 선택하도록 정부 기관에 권장해야 하며 벤더가 지속적인 제품 지원 및 업데이트에 대해 적절한 보상을 받도록 해야 합니다. 이러한 권고는 라이선싱 또는 개발 모델에 상관없이 모든 IT 솔루션에 똑같이 적용되어야 합니다. 지속적인 테스트로 강화되고 시장에서 입증된 상용 시스템은 대개 테스트되지 않은 맞춤형 접근 방식보다 더 안정적이고 안전한 것으로 입증됩니다. 오픈 소스 기술을 정부 IT 시스템에 통합할 수 있지만, 벤더에서 지속적인 보안 패치 및 업그레이드를 관리해 주는 지원으로 뒷받침하지 않는 한 이러한 시스템은 정부 네트워크에 위험을 초래할 수 있습니다.

클라우드 서비스의 보안 이점을 활용해야 합니다. 클라우드 컴퓨팅 서비스는 현대 경제의 중추(백본)로, 혁신적인 비즈니스 및 정부 솔루션을 강화하며 전례 없는 연결성, 생산성 및 경쟁력을 제공합니다. 또한 클라우드 서비스는 대개 정부가

---

2 John L. Gantz 외, "라이선스가 없는 소프트웨어 및 사이버 보안 위협", International Data Corporation 백서(2015년 1월) - http://globalstudy.bsa.org/2013/Malware/study_malware_en.pdf에서 확인할 수 있습니다.

사이버 보안 위협에 대한 태세를 개선하도록 도울 수 있는 보안 이점을 제공합니다. 이러한 이점을 활용하기 위해 정부는 클라우드 서비스로의 마이그레이션을 장려하는 정책을 채택해야 하며, 조달 정책을 현대화하여 클라우드 서비스가 공평한 경쟁의 장에서 경쟁할 수 있도록 해야 합니다. 기존의 구매 관행 및 계약 조건은 클라우드 컴퓨팅의 확장 가능하고 비용 효율적이며 혁신적인 특성을 저해할 수 있습니다. 부담스러운 조건으로 인해 방해받지 않는 빠르고 유연한 조달 프로세스를 통해 사용자는 클라우드 컴퓨팅 기술이 제공하는 다양한 이점을 최대한 활용할 수 있습니다.

인수 프로세스에 보안 고려 사항을 부가해야 합니다. 많은 국가에서 정부가 투자 가치를 극대화할 수 있도록 보장하는 규칙을 비롯하여 정부를 위한 제품 인수 안내 규정을 채택하고 있습니다. 경우에 따라 이러한 정당한 의도는 다른 상황과 상관없이 최저 가격을 제공하는 제품을 선호해야 한다는 지시로 이해되었습니다. 이러한 규칙으로 인해 정부 기관은 대개 정보 기술 조달의 맥락에서 해당 기관에 최고의 가치를 제공하는 제품 또는 서비스를 선택하지 못하게 됩니다. 그러한 추가 가치는 여러 다양한 방식으로 나타날 수 있습니다. 예를 들어 보안 강화, 추가 기능, 탁월한 제품 지원 또는 뛰어난 사용 편의성의 형태로 드러날 수 있습니다. 또한 이러한 규칙은 조달 프로세스의 한 요인으로 기관의 과거 실적에 대한 고려를 제한할 수 있습니다. 따라서 현실적으로 관련성이 높은 정보를 무시하게 될 수 있습니다. 이러한 규칙은 해당 솔루션이 가장 낮은 총 소유 비용을 제공하지 못하며 정부의 비용에 대해 최고의 가치를 제공하지 못하는 경우에도 정부 기관이 "가장 비용이 적게 드는" 솔루션을 선택하게 만드는 상당한 위험을 초래합니다. 대신, 정부는 "최고의 가치" 계약 정책을 채택해야 합니다. 이 정책에서는 정부가 투자 수익률을 극대화할 수 있도록 비용, 가치, 과거 실적, 보안 및 기타 변수에 따라 제안을 평가합니다.

IT 시스템을 스마트하고 안전하게 관리해야 합니다. 정부 IT 시스템의 사이버 보안에 대한 보장은 스마트한 구매 결정에 머물지 않습니다. 수명 주기 전체에 걸쳐 스마트한 시스템 관리가 필요합니다. 위협 환경이 변화함에 따라, 사이버 보안 기술의 지속적인 개발, 스마트한 관리, 일관된 계획 및 사이버 보안에 중점을 둔 IT 시스템에 대한 적절한 예산 책정이 필요합니다. 구체적으로 말하면 정부 기관의 IT 인수를 규정하는 정책은 다음을 준수해야 합니다.

» **소프트웨어 및 시스템을 최신 상태로 유지.** 여러 중대한 데이터 침해 시도에서는 오래되거나 패치되지 않은 소프트웨어 및 시스템을 활용합니다. 정부 기관은 최신 소프트웨어 및 시스템을 유지 관리하기 위한 계획을 수립하고 예산을 책정해야 합니다.

» **지속적인 보안 계획 수립.** 정부 기관은 너무도 자주 순수한 의도에서 해당 솔루션의 보안을 보장 및 유지할 계획 없이 특정 문제를 해결하기 위해 맞춤형 소프트웨어 솔루션을 구현하려고 합니다. 정부 기관은 해당 솔루션이 통합되기 전에 소프트웨어 및 IT 시스템의 업데이트/패치를 포함한 지속적인 보안 계획을 수립해야 하며, 이러한 계획은 제품 수명 주기 전체에 걸쳐 유지되어야 합니다. 또한 정부는 개발자, 엔지니어 및 관련 업무 종사자의 사이버 보안 역량에 투자함으로써 미래의 보안 요구에 부응하는 데 필요한 기술 및 직무 프로파일에서 혁신을 이끌어야 합니다.

» **SAM 통합.** 국제적으로 인정받은 표준 기반의 투명하고 검증 가능한 SAM(소프트웨어 자산 관리) 방침을 통해 정부 기관은 라이선스가 없는 소프트웨어(대개 패치되지 않고 취약성이 남아 있음)의 사용을 확인하고 그 문제를 해결하기 위한 조치를 취함으로써 IT 인벤토리를 보호할 수 있습니다.

국내 제품/서비스 선호 요구 사항을 피해야 합니다. 최첨단 제품 및 서비스는 여러 다양한 국가에 있는 연구 및 설계 센터의 전 세계적인 협업을 통해 개발됩니다. 각 국가는 국가 간 협업을 위한 장려책을 생성함으로써 정부의 인수 정책을 비롯하여 여러 방법을 통해 공유된 보안 과제에 대한 신속하고 혁신적인 솔루션을 촉진해야 합니다. 그러나 일부 국가에서는 대외 경쟁을 방지함으로써 국내 주요 기업을 보호하고 국내 토착 기술 산업을 발전시키며 외국 제품에서 인지된 사이버 보안 위험으로부터 방어할 수 있다고 가정하여 정반대의 접근 방식을 택하고 있습니다. 토착 기술은 글로벌 혁신의 일부분만 나타낼 뿐입니다. 정부 조달에서 대외 경쟁을 방지하면 정부 기관이 세계적 수준의 제품 및 서비스를 이용하지 못하게

거부함으로써 사이버 보안이 저하될 수 있습니다. 또한 이러한 정책은 국내 기술 기업이 글로벌 리더와 협업할 수 있는 소중한 기회를 박탈하고 국제 경쟁력을 약화시켜 글로벌 혁신을 저해합니다. 글로벌 시장에서 솔루션을 조달할 수 있도록 개방하면 효율성이 증대되고 비용이 절감되며 보안이 향상됩니다.

연구 및 개발

사이버 보안 기술 및 도구에 대한 연구 및 개발을 지원해야 합니다. R&D(연구 및 개발) 투자는 정부가 사이버 보안을 발전시킬 수 있는 구체적인 수단을 제공합니다. 이러한 R&D를 통해 정부가 기술 솔루션의 발전을 촉진함으로써 격차 및 당면 과제를 파악하는 것은 물론 광범위한 정부 시스템에 보안을 구축하기 위한 새로운 접근법을 개발할 수 있습니다. R&D 투자는 업계 및 학계의 국내 사이버 보안 에코시스템을 지원하는 데 도움이 됩니다. 또한 R&D 는 개별 기술을 넘어서서 사이버 보안을 향상시키기 위한 도구의 개발을 목표로 할 수 있습니다. 이러한 도구는 기존 기술의 새로운 응용 조사부터 국제적으로 인정받은 표준 및 특정 사이버 보안 과제에 대한 조직적 접근법을 안내하는 모범 사례 프레임워크의 개발 지원에 이르기까지 다양할 수 있습니다.

사이버 보안 및 민간 부문

중요 인프라

국가 사이버 보안 정책의 토대는 중요 인프라 전체에 걸쳐 사이버 보안을 보장하기 위한 프레임워크입니다. 대다수 국가에서 중요 인프라 운영자는 주로 민간 부문에 있기 때문에 이러한 프레임워크가 공공 부문과 민간 부문의 긴밀한 협업을 촉진하고 모든 이해 관계자의 요구 및 목표를 반영하는 것이 중요합니다.

보안 성과에 집중해야 합니다. 중요 인프라 부문은 대개 기술 인프라 측면에서 다양하고, 서로 다른 유형의 위험을 수반하며, 다양한 위협 및 위협 공격자에 직면해 있습니다. 게다가 이러한 인프라에 사용되는 기술은 다양하며 끊임없이 발전하고 있습니다. 구체적인 방법이나 엄격한 준수에 중점을 둔 지나치게 지시적인 규제 또는 보안을 개선시키기보다는 암호화와 같은 보안 강화 기술의 사용을 제한하는 명령은 적응형 보안 조치의 발목을 붙잡고 새로운 보안 기술의 혁신을 저해할 수 있습니다. 대신, 정부는 원하는 보안 성과를 끌어낸다는 측면에서 중요 인프라 사이버 보안 정책에 집중해야 합니다. 따라서 원하는 보안 성과를 달성할 수 있는 가장 효과적이고 혁신적인 접근법을 개발할 자유를 민간 부문의 법인에 제공해야 합니다. 위험 평가 도구, 성숙도 모델 및 위험 관리 프로세스를 통합하는 결과 기반 접근법을 통해 조직은 사이버 보안 활동의 우선순위를 정하고, 가장 긴급한 위험에 대한 방어를 조정하기 위해 정보에 근거하여 사이버 보안 리소스 할당에 대한 결정을 내릴 수 있습니다.

위험 기반의 유연한 정책 프레임워크를 사용해야 합니다. 기술은 빠르게 그리고 예측 불가능한 새로운 방향으로 발전합니다. 따라서 중요 인프라 사이버 보안을 위한 정책 프레임워크는 혁신 및 경제 발전을 저해하는 것을 방지하기 위해 충분히 상황에 맞춰 조정할 수 있는 보안 조치를 취하는 것이 필수적입니다. 이러한 균형을 이루기 위해 중요 인프라 사이버 보안 프레임워크는 다음과 같은 주요 원칙을 기반으로 해야 합니다.

1. **위험 기반 및 우선순위 지정.** 사이버 보안 위협은 다양한 심각도 단계의 여러 규모와 형태로 나타납니다. 객관적인 위험 평가(섹션 III, 정의 참조)에 따라 중요한 자산 및/또는 중요한 부문을 최우선으로 하여 우선순위 계층을 설정하는 것이 효과적인 출발점입니다. 이를 통해 피해 가능성이 가장 높은 해당 영역에 사이버 보호를 집중해야 합니다.
2. **기술 중립성.** 사이버 보안 보호에 대한 기술 중립적인 접근법은 시장에서 가장 안전하고 효과적인 솔루션에 대한 액세스를 보장하는 데 필수적입니다. 특정 기술만 사용하도록 지시하거나 사용하지 못하게 금지하는 특정 요구 사항 또는 정책은 보안 컨트롤(섹션 III, 정의 참조) 및 모범 사례의 발전을 제한하고 잠재적으로 단일 장애 지점을 생성함으로써 보안을 약화시킵니다.
3. **현실성.** 민간 운영자에 대해 지나치게 부담스러운 정부 감독 또는 사이버 보안 위험의 운영 관리에 대해

모범사례

중요 인프라 사이버 보안 개선을 위한 NIST 프레임워크

중요 인프라 사이버 보안 개선을 위한 NIST(미국 국립 표준 기술 연구소) 프레임워크는 사이버 보안 위험 관리에 대한 자발적인 위험 기반 접근법으로, 중요 인프라 운영자를 비롯하여 모든 규모 및 유형의 조직에 적용하고 확장하기 위한 것입니다. 이 프레임워크는 사이버 보안 위험 관리의 수명 주기 전체를 반영하는 5가지 핵심 기능 즉, 확인, 보호, 탐지, 대응 및 복구를 중심으로 구성됩니다. 이러한 기능들은 22가지 범주와 98가지 하위 지침 범주로 세분화되며, 이는 국제적으로 인정받은 표준(예: 정보 보안 관리 시스템 표준의 ISO/IEC 27000 시리즈) 과 기타 유용한 참조 기준에 대응됩니다. 이와 같은 프레임워크는

- ✅ 위험을 기반으로 하고 유연하며 결과 지향적이어야 합니다.
- ✅ 국제적으로 인정받은 표준 및 위험 관리 접근법에 맞춰 조정되어야 합니다.
- ✅ 공공 부문과 민간 부문의 파트너십을 포괄해야 합니다.
- ✅ 지역 고유 기술 표준에 대한 의존성을 피해야 합니다.
- ✅ 부담스러운 규제 제도를 피해야 합니다.

프레임워크는 중요 인프라 전반에 걸쳐 사이버 보안을 강화하기 위한 기본적인 사이버 보안 정책 접근법입니다. 실제로 미국 정부는 국방부 및 정보기관을 비롯한 모든 연방 정부 기관이 자체 위험 관리 프로그램을 안내하는 데 프레임워크를 사용하도록 지시했습니다. 이용 가능한 데이터에 따르면, 프레임워크는 중요 인프라 운영자에 의해 광범위하게 채택되었으며, 2020년까지 모든 미국 조직의 50% 이상이 이를 채택할 것으로 예상됩니다. 이탈리아의 국가 사이버 보안 프레임워크 및 말레이시아의 MDEC 사이버 보안 산업 개발 프레임워크와 같이 다른 몇몇 국가에서도 실질적으로 이와 비슷한 프레임워크 접근법을 채택하기 시작했습니다.

불균형적으로 강요하는 규제 개입은 대체로 역효과를낳는 것으로 드러났으며, 리소스 활용을 효과적이고 확장 가능한 보호에서 파편화된 관리 준수로 바꿔 놓습니다. 대신, 프레임워크는 대상 법인 전체에서 액세스 가능하고 확장 가능한 표준 및 보안 조치를 확립해야 합니다.

4. **유연성.** 사이버 위험 관리는 여러 분야에 걸쳐 있는 기능이며 보편적으로 적용할 수 있는 접근법이 없습니다. 각 산업, 시스템 및 비즈니스는 뚜렷한 과제에 직면해 있으므로 담당자의 업무 범위에 유연성이 있어야 합니다. 그래야 각각의 고유한 요구를 처리할 수 있습니다.

5. **개인정보보호 및 적법한 절차 존중.** 보안 요구 사항은 개인정보보호 및 적법한 절차 보호에 대한 요구와 충분히 균형을 이루어야 합니다. 요구 사항과 법적 의무는 비례적이고, 절대적으로 필요한 수준 이상으로 개인의 권리를 침해해서는 안 되며, 적법한 절차를 준수하고, 적절한 사법 감독의 지원을 받는 것은 모두 중요 인프라 사이버 보안 프레임워크에서 다루어야 하는 중요한 고려 사항입니다.

인증 제도는 소프트웨어 개발용 프로세스 기반 표준을 포함함으로써 소프트웨어 설계 단계부터 보안을 강조해야 합니다.

중요(정보) 인프라에 대한 너무 폭넓은 정의를 피해야 합니다. 폭넓은 정의는 준수와 관련하여 그리고 시행하는 동안 비즈니스 소유자, 해당 공급업체 및 정부 기관 간에 불확실성을 야기시킵니다. 이러한 정의는 실제로 사이버 보안을 개선하지 않으면서 비용이 많이 드는 규제 부담을 유발할 가능성이 높으며, 이로 인해 인프라 운영자는 실질적으로 필수적인 시스템을 지원하기 위해 처리해야 할 업무를 감당하지 못하게 됩니다. 또한 지나치게 광범위한 정의로 인해 규제 당국이 불필요한 정보 및 감독/시행 책임을 감당하지 못하게 될 수 있습니다. 대신, 정부는 실질적으로 필수적인 시스템에 집중하는 중요(정보) 인프라 (섹션 III, 정의 참조)의 정의를 채택하고, 엄격하고 균형 잡힌 위험 기반 분석을 적용하여 구체적으로 무엇을 중요(정보) 인프라로 지정해야 하는지 결정해야 합니다.

국제적으로 인정받은 표준에 맞춰 중요 인프라 보안을 조정해야 합니다. 표준 및 모범 사례는 민간 부문과의 협업을 통해 개발되고 자발적으로 채택되며 전 세계적으로 인정받을 때 가장 효과적입니다. 정부가 중요 인프라 사이버 보안 문제를 해결하기 위해 발표한 규정, 정책 및 표준은 정보 보안(섹션 III, 정의 참조) 관리 표준에 대한 ISO/IEC 27000 및 ISO/IEC 62443 시리즈와 같이 국제적으로 인정받은 위험 관리 접근법 및 국제적으로 인정받은 기술 표준(섹션 III, 정의 참조), 정보 기술 보안 평가를 위한 공통 기준 또는 중요 인프라 사이버 보안 개선을 위한 NIST 프레임워크에 맞춰 적절하게 조정해야 합니다. 정부는 특히 자발적인 합의 기반 프로세스를 통해 개발된 해당 표준에 맞춰 조정해야 한다는 사실을 강조해야 합니다. 중요 인프라 운영자가 발전하는 모범 사례 및 표준을 사용하여 진화하는 사이버 보안 위협에 대처할 수 있게 한다면 사이버 보안에 대한 더 유연한 최신 위험 기반 접근법이 가능해집니다. 게다가 국제적으로 인정받은 표준을 사용하면 국제적인 상대와 기업 및 정부 기관의 상호 운용성이 보장되므로 사이버 보안 위협에 맞서 경제 발전 및 운영 협업을 모두 촉진할 수 있습니다.

지역의 고유한 보안 표준을 피해야 합니다. 일부 정부는 중요 인프라 사이버 보안에 대한 국가별 표준을 시행하고 있으며, 시장별 규칙을 적용하면 사이버 보안이 향상될 것이라고 주장합니다. 그러나 실제 효과는 정반대입니다. 정부에서 시행하며 전 세계적으로 용인되는 모범 사례 및 표준과 일치하지 않는 지역의 고유한 표준은 보안을 강화하는 대신, 혁신을 저해하고 소비자와 기업이 자신의 요구에 부합되지 않는 제품을 사용하게 만드는 경향이 있습니다. 이러한 접근법은 중요 인프라가 최고 수준의 솔루션을 대표하는 보안 기술을 통합하지 못하게 만들 수 있습니다.

인증 제도는 균형적이고 투명하며 국제적 기준을 따라야 합니다. 인증 제도(섹션 III, 정의 참조)는 중요 인프라 커뮤니티에서 더 강력한 사이버 보안을 촉진하는 효과적인 방법일 수 있지만, 보안 요구를 촉진하고 지속적인 혁신과 제품 유형 및 구성의 광범위한 다양성에 대한 시장 요구를 해결하는 방식으로 구조화되어야 합니다. 따라서 모든 인증 제도는 국제적으로 인정받은 표준 또는 위험 관리 접근법 (예를 들어 정보 보안 관리 표준에 대한 ISO/IEC 27000 및 ISO/IEC 62443 시리즈 또는 중요 인프라 사이버 보안 개선을 위한 NIST 프레임워크가 있으며, 둘 다 위험 관리 및 전 세계 주요 인프라 운영자의 사이버 보안 개선에 널리 사용됨)을 기반으로 해야 합니다. 이러한 국제적 접근법은 표준 및 위험 관리 방침의 지속적이고 반복적인 개발을 특징으로 하는데, 이러한 특징을 통해 인증 프레임워크는 기술 발전에 따라 최신 상태를 유지하고 정부 및 민간 부문 이해 관계자의 조언 및 모범 사례를 전 세계적으로 통합할 수 있습니다. 인증 제도는 ISO/IEC 27034 표준 시리즈와 같은 개발 프로세스 전반에 걸쳐 보안 고려 사항을 통합하는 소프트웨어 개발용 프로세스 기반 표준을 포함함으로써 소프트웨어 설계

모범사례

인증 제도는 자발적이고, 시장 중심적이며, 광범위하고, 국제 기준을 따라야 합니다.

제품 인증 또는 라벨 부착 제도는 소비자 인식을 개선하고 더 강력한 사이버 보안 제품을 촉진하는 효과적인 방법일 수 있지만, 지속적인 혁신과 제품 유형 및 구성의 광범위한 다양성에 대한 시장 요구를 반영하는 방식으로 구조화되어야 합니다. 따라서 인증 및 라벨 부착 제도는 국제적으로 검증되고 인정받은 표준과 연계된 자체 평가 제도를 비롯하여 자발적인 합의 기반의 업계 주도 이니셔티브에만 엄밀하게 중점을 두어야 합니다. 또한 자발적인 합의를 기반으로 업계가 주도하는 표준 설정 프로세스를 사용할 경우 해당 접근법이 광범위하게 채택되지 않으면 효과적인 접근법이 될 수 없습니다. 인증 또는 라벨 부착 표준을 채택하도록 시장 중심으로 장려하는 방식이 다른 대안보다 더 낫습니다. 법규를 통해 채택을 요구하거나 보험 시장 및 법적 책임을 형성하는 데 채택을 사용할 경우 유연하고 결과 지향적인 표준을 저해하고 혁신을 약화시키는 의도하지 않은 결과를 초래할 수 있습니다. 대신, 정부는 인증 제도 참여를 유도하는 시장 중심의 장려책을 만들어야 합니다.

단계부터 보안을 내재화하는 원칙(Security-by-Design) 을 강조해야 합니다. 이러한 프로세스 기반 접근법은 처음부터 보안을 통합하는 중요성을 인식하지만, 최신 소프트웨어 개발의 민첩하고 반복적인 특성도 고려합니다. 게다가 중요 인프라 부문에서 사용되는 인증 제도는 (1) 투명해야 합니다. 즉, 중요 인프라를 운영하는 기업 또는 중요 인프라 운영자에게 제품 또는 서비스를 제공하는 기업이 인증 표준, 방법론, 프로세스 및 결과를 완벽하게 파악할 수 있어야 합니다. 그리고 (2) 독립적이어야 합니다. 즉, 특정 국내 법인의 독점적 사용을 요구하는 대신, 국제적으로 승인받은 인증 기관의 사용을 허용해야 합니다.

소스 코드 및 기타 지적 재산의 공개 요구를 거부해야 합니다. 일부 국가에서는 특정 제품의 개발자가 해당 제품을 중요 인프라에 사용하려면 먼저, 검사를 위해 소스 코드 및 관련 지적 재산을 제공해야 한다는 법률을 시행하기 시작했습니다. 이러한 요구는 부적절하고 효과가 없습니다. 소스 코드, 기업 표준, 보안 테스트 결과 및 이와 유사한 독점 정보를 공개하도록 요구하는 것은 지적 재산 보호에 상당한 내재적 위험을 야기하지만 보안의 부가 가치는 거의 제공하지 않습니다. 오늘날 많은 기술 제품에는 수십만 또는 수백만 라인의 코드가 포함되어 있기 때문에 검사관은 그야말로 간단히 단일 코드의 결함을 확실하게 파악하지 못합니다. 정부가 소프트웨어 개발자가 공개한 코드를 보관하는 경우 해당 코드는 해커의 절도 표적이 될 수 있으며 잠재적으로 공격자가 공격 방법을 알아내고 개선하는 데 사용될 수 있습니다. 정부는 어떠한 법률을 통해서도 그러한 소프트웨어 또는 해당 소프트웨어가 포함된 제품의 수입, 유통, 판매 또는 사용을 위한 조건으로 소스 코드의 이전 또는 소스 코드에 대한 액세스를 요구하지 않아야 합니다.

소비자 제품

시장 중심 솔루션을 촉진해야 합니다. 기술, 보안 접근법 및 소비자 요구가 끊임없이 변화하기 때문에 필요 이상으로 엄격한 규제 접근법은 시장의 역동성 및 다양성을 미처 따라가지 못합니다. 대신, 소비자 시장에서 사이버 보안을 증진하는 가장 효과적인 방법은 시장의 힘을 활용하여 더

강력한 보안을 촉진하는 것입니다. 시장 중심 솔루션은 업계 주도하에 국제적으로 인정받은 표준의 개발 및 채택, 산업 컨소시엄, 세제 혜택, 책임 면제, 자발적 인증 및 라벨 부착 제도를 비롯하여 다양한 형태로 제공됩니다. 소비자 제품의 사이버 보안 문제에 대처하기 위해 정책 프레임워크를 생성할 때 각국 정부는 자체적으로 고유한 상황에 맞게 조정한 시장 중심 솔루션을 채택하고 의무적인 규제 조치를 피해야 합니다.

국제적으로 인정받은 표준의 채택을 장려해야 합니다.

기술 표준(섹션 III, 정의 참조)은 사이버 보안을 활성화하고 강화하는 데 필수적인 역할을 합니다. 업계의 참여를 통해 개발되고 시장 전반에 걸쳐 수용되는 국제적으로 인정받은 기술 표준을 지원함으로써 기업은 더 새롭고 안전한 제품을 더 신속하게 개발, 유통 및 채택할 수 있습니다. 게다가 국제적으로 인정받은 표준을 사용하면 국제적인 상대와 기업 및 정부 기관의 상호 운용성이 보장되므로 사이버 보안 위협에 맞서 경제 발전 및 운영 협업을 모두 촉진할 수 있습니다. 따라서 정부는 소비자 제품의 사이버 보안에 관한 규정, 법률 또는 정책을 국제적으로 인정받은 기술 표준과 국제적으로 인정받은 위험 관리 접근법에 맞춰 조정해야 합니다.

데이터 흐름

비즈니스 목적의 국가 간 데이터 흐름을 지원해야 합니다.

현대 경제는 클라우드 컴퓨팅 서비스 및 기타 기술을 사용하여 여러 위치와 국경을 넘나드는 데이터를 저장, 처리 및 전송할 수 있도록 지원합니다. 이러한 기술은 여러 시장 간에 데이터가 자유롭게 흐르도록 함으로써 국제 무역, 국가 간 비즈니스 협업 및 규모의 경제를 추동하고 전 세계적인 전염병, 재난 대응 등의 일반적인 거버넌스 문제에 대한 기술 솔루션 적용을 점점 더 촉진합니다. 게다가 이러한 기술은 안정성, 복원력, 24시간 보안 지원 등의 보안상의 이점을 제공합니다. 비즈니스 목적의 국가 간 데이터 전송을 제한하는 법률은 경제적 이점과 보안 이점을 모두 저해하므로 국가 사이버 보안의 법적 및 정책 프레임워크에서는 피해야 합니다.

- **개인정보보호, 보안 및 국가 간 데이터 흐름 촉진.** 일부 국가의 사이버 보안 제도에서는 개인정보보호나 보안 목적으로 또는 둘 모두를 위한 목적으로 데이터 보호 목표를 달성하기 위해 국가 간 데이터 흐름에 대한 제한을 설정했습니다. 그러나 이러한 제한은 효과적인 데이터 보안을 달성하는 데 부적절하며 대개 역효과를 낳습니다. 국가 간 데이터 규칙에 대해 집행 가능한 국제 합의가 존재하는 것은 아니지만, 책임감 있는 데이터 관리는 OECD(경제협력개발기구)의 "개인정보 및 국가 간 개인 데이터 흐름의 보호에 대한 지침"에 명시된 대로 그리고 APEC(아시아 태평양 경제협력체) 개인정보보호 프레임워크와 같은 프레임워크에서 구체화된 대로 투명성 및 책임성에 대해 국제적으로 인정받은 원칙을 기반으로 해야 합니다.
- **데이터 프로세서와 데이터 컨트롤러 구별.** 개인 데이터 보호 제도에서는 데이터 주체 또는 소유자에 대한 책임 및 의무를 명확히 하고 더불어 법적 요구 사항 준수를 촉진하기 위해 데이터 컨트롤러와 데이터 프로세서를 구별하는 것이 중요합니다. 데이터 컨트롤러는 개인 데이터와 관련된 의무를 준수할 책임이 있는 법인이어야 합니다. 데이터 프로세서는 데이터 컨트롤러를 대신하는 역할만 합니다. 데이터 프로세서는 데이터 컨트롤러가 부여한 권한을 기반으로 데이터를 취급합니다. 따라서 일반적으로 조치에 따라 데이터 프로세서의 의무가 명확히 제한된 계약에 의해 데이터 프로세서의 의무를 규정해야 합니다.

> **정부는 소비자 제품의 사이버 보안에 관한 규정, 법률 또는 정책을 국제적으로 인정받은 기술 표준과 국제적으로 인정받은 위험 관리 접근법에 맞춰 조정해야 합니다**

데이터 현지화 요구 사항을 피해야 합니다. 데이터가 특정 위치에서 더 안전하다는 잘못된 가정에 따라 몇몇 국가에서는 데이터를 국내에서 보관해야 하는 규칙을 시행하고 있습니다. 실제로 데이터 현지화 요구 사항은 현대 경제를 뒷받침하는 클라우드 컴퓨팅 서비스와 기타 기술의 이점을 훼손함으로써 글로벌 무역을 저해할 뿐만 아니라, 이러한 기술을 통해 얻을 수 있는 많은 보안 이점(예: 이중화, 24시간 보안 모니터링, 클라우드 기반 네트워크 방어 도구 등)을 무시하게 됩니다. 데이터 현지화 요구 사항은 사이버 보안에 대한 가장 비생산적인 접근법 중 하나이므로 거의 모든 상황에서 피해야 합니다.

신기술을 사용할 수 있도록 지원하는 정책 환경을 유지해야 합니다. 신기술은 점점 더 중요한 사이버 보안 도구가 되고 있습니다. 예를 들어 AI(인공 지능) 지원 사이버 도구를 사용함으로써 분석가는 하루에 수십만 건의 보안 사고를 분석하여 가양성을 제거하고 네트워크 관리자가 다시 확인해야 하는 위협을 파악할 수 있습니다. 사이버 보안 위협은 전 세계에서 발생하기 때문에 AI 지원 사이버 도구를 훈련시키는 데 사용되는 데이터는 국경을 넘어 이동할 수 있어야 합니다. 또한 데이터 전송을 금지하는 정책 또는 트래픽 데이터를 분석하여 위협을 파악하는 기능을 제한하는 정책은 사이버 보안을 위한 신기술의 사용을 방해하게 됩니다.

사이버 보안 및 시민

인식

공공의 사이버 보안 인식에 투자해야 합니다. 대다수의 사이버 침해 및 공격은 개개인의 사이버 예방 조치가 열악한 것에 기인합니다. 정부가 컴퓨터 및 네트워크를 보호한다는 측면에서 정부 및 시민의 공동 역할에 대한 대중의 인식을 제고하는 데 투자하면 사회 전반의 사이버 보안 및 사이버 복원력을 촉진할 수 있습니다. 정부는 다양한 방법으로 대중의 인식 제고에 투자할 수 있습니다. 예를 들어 성공적인 활동에는 전국적인 인식 제고 행사(예: 주간 또는 월간 국가 사이버 보안 인식 제고), 공공 서비스 광고 캠페인, 전용 웹 사이트 및 온라인 지침, 소셜 미디어 캠페인, 학교 행사 등이 포함됩니다. 정부가 사이버 보안 인식을 증진할 수 있는 또 다른 중요한 방법은 연구원, 정책 입안자 및 일반 시민이 사이버 보안 사고에 대해 공개된 종합 데이터를 사용할 수 있게 함으로써 사이버 보안 당면 과제의 범위 및 윤곽을 더 잘 이해할 수 있도록 하는 것입니다.

소비자 선택에 영향을 미치는 도구를 만들어야 합니다. 사이버 보안을 향상시키는 데 있어서 중요한(그러나 대개 무시되는) 요소는 개별 및 기업 소비자 모두가 보안 제품과 보안 서비스를 채택하도록 촉진하는 것입니다. 대부분의 경우 소비자는 정보에 근거하여 보안 기반 제품을 구별하여 의사 결정을 내리는 역량이나 보안 제품 또는 서비스의 비교 가치를 이해하는 능력이 부족합니다. 정부는 사이버 보안 인식을 강조하고 소비자가 시장에서 중요한 제품 보안 정보를 취득 및 비교하는 데 사용할 수 있는 도구를 개발함으로써 사이버 보안 향상을 지원할 수 있으며, 소비자가 정보 기술 에코시스템 전반의 사이버 보안 강화에 기여하도록 지원할 수 있습니다.

인력 개발

모든 수준의 교육에서 사이버 보안 인식을 증진해야 합니다. 현재와 미래의 요구에 부응하기 위한 사이버 보안 인력 풀을 구축하는 작업은 광범위한 세대의 미래 전문가를 교육하는 것으로 시작됩니다. 정부는 교육 시스템의 모든 수준에서 사이버 보안 교육을 이용 가능하고 접근 가능하며 사이버 보안 인력의 요구와 새로운 사이버 보안 과제 모두에 맞춰 조정할 수 있는 프로그램에 투자해야 합니다. 정부는 (1) 청소년이 초등학교 교육과정을 통해 기초적인 사이버 예방 조치를 비롯한 사이버 보안 개념을 접하게 하는 프로그램, (2) 장학금 및 연구 경연 대회를 통해 청소년 사이에 사이버 보안 교육에 대한 관심 및 접근을 증대하는 프로그램 그리고 (3) 대학교, 지역 대학 및 기타 교육의 장을 통해 사이버 보안 중심의 교육 프로그램을 개발, 승인 및 촉진하도록 장려하는 프로그램을 고려해야 합니다.

사이버 보안 교육 및 훈련에서 다양성의 우선순위를 정해야 합니다. 전 세계적으로 여성 및 소수 민족은 사이버 보안 인력에서 그다지 두각을 나타내지 못하는 경향이 있는데, 이는 노동력 풀의 상당한 부분을 차지하고 있는 여성 및 소수 민족의 재능 및 관점을 활용하지 못함을 나타냅니다. 정부가 미래의 사이버 보안 전문가에게 교육을 제공하기 위해 더 광범위한 활동에 투자할 때 그러한 프로그램을 통해 더 많은 여성과 소수

사이버 보안의 일자리 공백 즉, 공석과 그 빈 일자리를 채울 수 있는 자격이 있는 개인 간의 격차가 계속 커질 때 도시와 시골 지역 출신의 재능 있는 젊은 여성 및 소수 민족 학생의 활기 넘치는 커뮤니티가 그 수요를 충족하는 데 도움이 될 수 있습니다 단, 정부가 이 필수적인 분야에 이들을 유치하고 고용하기 위한 스마트한 정책을 채택해야 합니다

민족의 학생들이 사이버 보안 교육을 이수하도록 장려해야 합니다. 또한 정부는 투자 시 도시의 수도와 산업 중심지 이외에서도 사이버 보안의 교육 및 취업 기회를 광범위하게 이용할 수 있게 만드는 것을 목표로 삼아야 합니다. 사이버 보안의 일자리 공백 즉, 공석과 그 빈 일자리를 채울 수 있는 자격이 있는 개인 간의 격차가 계속 커질 때 도시와 시골 지역 출신의 재능 있는 젊은 여성 및 소수 민족 학생의 활기 넘치는 커뮤니티가 그 수요를 충족하는 데 도움이 될 수 있습니다. 단, 정부가 이 필수적인 분야에 이들을 유치하고 고용하기 위한 스마트한 정책을 채택해야 합니다.

사이버 보안 취업을 위한 대체 경로를 지원해야 합니다. 사이버 보안 전문 지식은 학사 또는 석사 학위가 필요하지 않은 대체 경로를 통해 즉, 수습직 프로그램, 지역 대학, 사이버 보안 "부트캠프" 또는 단기 집중 교육 아카데미, 관련 정부 또는 군 서비스 등을 비롯하여 다양한 방법을 통해 개발할 수 있습니다. 정부는 이러한 대체 경로를 육성하는데 투자해야 합니다. 또한 미래의 사이버 보안 일자리를 채우기 위해 젊은이의 교육에 투자하는 것이 중요합니다. 하지만, 디지털 상거래의 성장이 빠른 속도로 진행되어 단기적으로 새로운 사이버 보안 전문가의 유입이 필요한 상황입니다. 중간 경력의 직장인이 사이버 보안 직업으로 전환할 수 있도록 지원하는 재교육의 기회에 투자하면 단기적으로 사이버 보안 인력 부족을 메우는 동시에 커뮤니티 발전을 통해 21세기 경제의 변화하는 인력 수요를 지원할 수 있습니다.

형사 법규

사이버 범죄

사이버 범죄에 대한 부다페스트 협약과 일관된 포괄적인 법적 프레임워크를 확립해야 합니다. 국가는 사이버 영역에서의 형사 책임, 수사 및 기소를 다루는 포괄적인 법규를 제정해야 합니다. 각국은 사이버 범죄(섹션 III, 정의 참조)에 대한 포괄적인 국가 법규를 개발하기 위한 가이드라인을 제공하는 사이버 범죄에 대한 부다페스트 협약[3]에 따라 그리고 이 조약의 당사국 간 국제 협력에 대한 프레임워크로서 해당 법규를 제정해야 합니다. 협약에는 실체법에 대한 요구 사항(범죄 대상에 대한 최소 기준), 절차적 메커니즘(조사 방법) 및 국제적인 사법 공조 (예: 디지털 증거에 대한 국가 간 접근 또는 범인 인도)가 포함됩니다. 법적 프레임워크에서는 국가 간 조사에 대한 지원을 규정해야 합니다.

범죄 의도가 있는 공격자에게만 형사 책임을 적용해야 합니다. 악의적인 공격자는 대개 개별 컴퓨터부터 주요 네트워크에 이르기까지 다양한 민간 소유 사이버 자산의 취약성을 악용하여 사이버 범죄를 저지릅니다. 예를 들어 상당히 심각한 사이버 보안 위협 중 하나인 봇넷은 수천 대의 개별 컴퓨터를 멋대로 사용하여 다른 시스템이나 네트워크 성능을 저하시키는 작업을 수행하도록 명령합니다. 악의적인 공격자가 사이버 공격(섹션 III, 정의 참조)의 일부로 민간 소유 자산의 사이버 취약성을 악용하는 경우 해당 자산의 소유자는 공격의 표적이자 공격의 피해자입니다. 범죄자는 그러한 취약성을 악용하는 악의적인 사이버 공격자입니다. 따라서 악의적인 활동의 피해자가 아닌 사이버 공간을 중단, 방해 또는 불안정하게 만들려는 사람들을 형사 기소해야 합니다.

3 2004년 1월 7일에 발효된 유럽 평의회의 사이버 범죄에 대한 협약(CETS No. 185)은 https://www.coe.int/en/web/cybercrime/the-budapest-convention 에서 확인할 수 있습니다.

> **전략 문서, 조직 및 예산에서 정부는 강력하고 협력적인 사이버 보안을 국가 안보의 중대한 요소로 강조해야 하며, 협력을 촉진하기 위해 집중해야 할 명확한 영역을 개발하고 분명히 설명해야 합니다.**

또한 형사 법규에서는 악의적인 공격자의 불법 활동과 보안 전문가가 사이버 보안 강화를 위해 설계한 합법적인 조사 및 테스트(관련 도구 및 기법을 사용할 수 있음)를 구별해야 합니다.

법 집행을 위한 기술 교육 및 지원을 제공해야 합니다. 디지털 기술이 지속적으로 발전함에 따라 전 세계 법 집행 조직은 기술 혁신에 맞춰 특히, 사이버 범죄를 효과적으로 조사 및 기소할 수 있도록 조사 기법을 계속 조정해야 합니다. 정부는 법 집행 조직이 기술 변화에 따라 충분한 조사 역량을 유지할 수 있도록 전문화된 사이버 단체의 설립을 비롯하여 적절한 기술 교육 및 기술 지원을 제공할 수 있는 메커니즘을 고려해야 합니다. 정부는 법 집행을 위한 액세스를 지원하는 기술 사양을 요구하는 정책을 피해야 합니다. 그러한 기술 사양은 사이버 보안을 약화할 수 있기 때문입니다.

국제 협정

국제 사이버 보안 협력 촉진

외교 정책에 사이버 보안 협력을 통합해야 합니다. 사이버 보안은 국제 협력 솔루션이 요구되는 초국가적인 과제입니다. 이러한 협력은 상황을 앞서서 주도하는 실질적인 외교를 통해 이루어집니다. 정부는 사이버 보안 관련 국제 협력에 대한 참여를 표명하고 이를 외교 정책의 주요 우선순위로 인식해야 합니다. 전략 문서, 조직 및 예산에서 정부는 강력하고 협력적인 사이버 보안을 국가 안보의 중대한 요소로 강조해야 하며, 협력을 촉진하기 위해 집중해야 할 명확한 영역을 개발하고 분명히 설명해야 합니다. 이러한 중점 영역에는 특정 사이버 보안 위협에 대처하기 위한 다국적 운영 협업 참여, 국제 사이버 보안 규범 또는 신뢰 구축 조치에 대한 지원, 외국 파트너의 사이버 보안 역량 구축, 국제 사이버 보안 표준 개발 참여 또는 다자간 거버넌스 메커니즘 참여가 포함될 수 있습니다. 또한 일부 정부는 사이버 보안 외교관 임명을 통해 이러한 영역 전반에 걸쳐 외교 활동을 집중하고 동기화할 수 있습니다.

국제 협력 활동에 참여해야 합니다. 국제 사이버 보안 협력은 2가지 중요한 영역 즉, 다자간 거버넌스 활동과 운영 협업에 뿌리를 내리고 있습니다. 다자간 거버넌스를 통해 각국 정부는 보안을 강화하고 경제적 연계를 심화하기 위한 공동 토대 역할을 하는 공통의 정책 및 표준을 개발할 수 있습니다. 각국은 국제 정책 및 표준 조직, COE(Centers of Excellence), 지역 및 국제 행사, 정부 간 논의, 공공 및 민간 연합, 기타 협업 메커니즘을 비롯한 국제 포럼 및 협력 메커니즘을 통해 공통의 통행 규칙, 협력 및 사고 대응 프로토콜, 공유 표준, 공통 인프라 등을 개발함으로써 운영 협업이 가능합니다. 법 집행 수사에 대한 협업 또는 초국가적인 영향을 미치는 사이버 보안 사고에 대한 대응과 같이 특정 사고 또는 위협을 해결하기 위한 실시간의 실질적인 협력 즉, 운영 협업을 통해 각국 정부는 잠재적인 위협 및 취약성에 대한 정보를 적시에 받고 결과적으로 모든 사고에 신속하게 대응할 수 있습니다. 정부는 두 가지 유형의 협업 모두에 참여하여 이러한 다자간 프레임워크의 맥락 내에서 요구 및 우선순위를 처리해야 하고 악의적인 사이버 활동으로부터 글로벌 네트워크를 방어하는 공동 책임을 지지해야 합니다.

수출 통제 정책이 합법적인 사이버 보안 활동을 저해하지 않도록 해야 합니다. 악의적인 침입, 악용, 취약성 및 기타 새로운 사이버 보안 위협으로부터 중요 네트워크 및 인프라를 보호하려면 실시간 테스트 및 수정 작업이 필요합니다. 빠르게 진화하는 위협 환경에 대처하기 위해 사이버 보안 전문가는 새로운 위협 및 솔루션에 대한 정보를

전 세계의 대규모 전문가 커뮤니티와 자유롭게 공유할 수 있어야 합니다. 네트워크 방어자는 방어하려고 하는 정확한 위협과 많은 기술적 특성을 공유하는 기술을 활용할 수 있어야 합니다. 예를 들어 사이버 보안 전문가는 "침투 테스트" 도구를 활용하여 네트워크가 기존/신규 소프트웨어 악용 및 해킹 기법에 취약한지 여부를 평가합니다. 해당 네트워크 취약성을 효과적으로 완화하기 위해 기업은 취약성 및 악용에 대한 정보를 자유롭게 그리고 실시간으로 공유할 수 있어야 합니다. 침투 테스트 도구에서 사용하는 취약성 및 악용의 실시간 공유를 금지하는 수출 통제는 안전한 제품을 만들고 보안 네트워크 및 IT 환경을 보장하는 능력에 심각한 영향을 미칩니다. 따라서 수출을 통제하여 악성 소프트웨어의 확산을 규제하려는 활동은 그 폭을 좁게 조정하여 사이버 보안 전문가, 사고 대응 담당자 또는 독립적인 연구 커뮤니티에 의도하지 않은 제한을 가하지 않도록 해야 합니다.

국제 사이버 보안 협력 촉진

해당 영역이 국제 사이버 공격에 사용되지 않도록 해야 합니다. 사이버 공격으로부터 고유한 시스템 및 네트워크를 방어하는 것 외에도 각국 정부는 악의적인 사이버 공격자가 다른 국가에 대한 사이버 공격을 시작 또는 지원하는 데 해당 국가의 영역을 사용하지 못하게 해야 할 책임이 있습니다. 악의적인 사이버 활동을 법으로 금지하는 법적 프레임워크는 피해자가 국경 너머에 있는 경우에도 이러한 활동을 포괄해야 합니다. 또한 국제 사이버 공격에 관련된 사람들을 파악하고 중단시킬 만큼 충분한 집행 메커니즘을 시행해야 합니다.

인터넷에서 개인정보 및 인권을 보호해야 합니다. 정부는 인터넷에 대한 액세스를 촉진하고 인터넷에서 표현할 권리를 보호하며 디지털 통신 시 개인정보를 보호하고 개인정보 또는 인권을 침해당한 개인이 적절한 법적 구제 방법을 사용할 수 있도록 하는 법률을 비롯하여 인터넷에서 인권 및 개인정보를 보호하는 UN 결의안을 이행하기 위한 법률을 통과시켜야 합니다. 그뿐만 아니라 정부는 개인정보보호 향상 기술의 개발 및 사용을 저해하는 정책을 피해야 합니다.

IT 시스템 제조업체가 국가 후원 해킹을 지원하게 만드는 명령을 피해야 합니다. 스파이 행위 및 기타 국가 후원 사이버 활동이 많은 정부에 의해 수행되지만, 정부가 기술 제공자에게 그러한 활동을 지원하게 하거나 그러한 활동에 동참하도록 만드는 시도는 국제 무역에 엄청나게 부정적인 결과를 야기할 수 있습니다. 따라서 정부는 정부 액세스 기능(대개 "백도어" 라고 함)을 지시하거나 암호화 키 또는 소스 코드 공개를 요구하거나 정보기관과의 협력을 요구하거나 범죄 혐의자에 대해 합법적으로 승인된 감시의 맥락을 벗어난 시민의 감시를 요구하는 등 기술 제공자가 국가 후원 사이버 활동을 지원하도록 명령하는 법률을 피해야 합니다.

섹션 III. 정의

인증 . 인증 인증은 “제품, 프로세스, 시스템 또는 사람과 관련하여 지정된 요구 사항이 충족되었음을 나타내는 제3 자 증명(즉, 명세서 발급)”으로 정의할 수 있습니다.

민간 법인. 민간 법인은 “법 집행, 정보 수집 또는 분석, 방위 또는 군대에 대한 주요 책임이 없는 정부 조직 또는 정부 후원 조직”으로 정의할 수 있습니다.

컴퓨터 데이터. 사이버 범죄에 대한 부다페스트 협약에 따라 컴퓨터 데이터는 “컴퓨터 시스템이 기능을 수행하게 하는 데 적합한 프로그램을 비롯하여 사실, 정보 또는 개념을 컴퓨터 시스템에서 처리하기에 적합한 형태로 표현한 것”으로 정의할 수 있습니다.

컴퓨터 시스템. 사이버 범죄에 대한 부다페스트 협약에 따라 컴퓨터 시스템은 “프로그램에 의하여 데이터 자동 처리를 수행하는 장치 또는 상호 연결되거나 관련된 장치 그룹”으로 정의할 수 있습니다.

지속적인 모니터링. 지속적인 모니터링은 “정보 시스템 내에서 계획, 요구 및 배포된 보안 컨트롤의 전체 세트가 시간 경과에 따라 변화하는 정보 기술 및 위협의 발전과 비교하여 계속 효과를 발휘하는지 확인하는 데 사용하는, 진행 중이거나 거의 실시간 프로세스”로 정의할 수 있습니다.

보호 조치. 보호 조치는 “사이버 보안 위협으로부터 정보 시스템을 보호하기 위한 것으로, 정보 시스템에 저장되거나 정보 시스템에 의해 처리되거나 정보 시스템을 통과하며 사이버 보안 위협의 지표를 포함하고 있는 것으로 알려졌거나 의심되는 정보를 수정, 리디렉션 또는 차단하는 자동화된 조치 또는 수동 조치”로 정의할 수 있습니다. 보호 조치는 다음과 같은 정보 시스템에서 수행하는 방어 조치입니다.

» 보호받는 당사자가 소유 또는 운영하는 정보 시스템

» 보호받는 당사자 대신 운영하는 정보 시스템 또는

» 보호받는 당사자에게 전자 통신 서비스, 원격 컴퓨팅 서비스 또는 사이버 보안 서비스를 제공하는 민간 법인이 운영하는 정보 시스템

중요 정보. 인프라 중요 인프라와 마찬가지로 중요 정보 인프라의 정의는 맥락 및 사용 의도에 따라 수정해야 할 수 있습니다. 일반적으로 중요 정보 인프라는 다음과 같이 정의할 수 있습니다.

> “중요 정보 인프라는 중요 인프라 자체이거나 중요 인프라의 운영에 필수적인 정보 및 통신 기술 시스템을 나타내며, 해당 시스템이 파괴되거나 저하되거나 사용 불가능하게 되면 국가 안보, 공중 보건, 공공 안전, 국가 경제 안보 또는 핵심 정부 기능이 약화되는 커다란 영향을 받습니다.”

중요 인프라. 중요 인프라에 대한 정의는 용어가 사용되는 맥락에 따라 광의로 적용하거나 협의로 적용할 필요가 있습니다. 또한 용어의 법적 정의를 넘어 국가 정부는 특정 중요 인프라 자산, 서비스 및 시스템을 파악하기 위한 위험 기반 프로세스를 유지해야 합니다. 그러나 일반적으로 중요 인프라는 다음과 같이 정의할 수 있습니다.

> “중요 인프라는 물리적이든 가상이든 그 유형에 상관없이 자산, 서비스 및 시스템을 의미하며, 이

인프라가 파괴되거나 저하되거나 장기간 사용 불가능하게 되면 국가 안보, 공중 보건, 공공 안전, 국가 경제 안보 또는 핵심 정부(주 또는 연방) 기능이 약화되는 커다란 영향을 받습니다. 구체적인 중요 인프라는 중요성, 상호 의존성 및 위험에 대한 분석을 기반으로 파악할 수 있습니다."

사이버 공격. 사이버 공격은 "정보 시스템에 저장되거나 정보 시스템에 의해 처리되거나 정보 시스템을 통과하는 정보 또는 정보 시스템의 보안, 가용성, 기밀성 또는 무결성에 악영향을 미치려고 하는 행위"로 정의할 수 있습니다.

사이버 범죄. 사이버 범죄에 대한 부다페스트 협약에 따라 사이버 범죄는 다음과 같이 정의할 수 있습니다.

"데이터 및 시스템의 기밀성, 무결성 및 가용성에 대한 범죄적 위법 행위 또는 시스템에 대한 무단 액세스로, 의도적으로 행하는 경우 다음 행위가 포함됩니다."

1. 불법적인 액세스: 컴퓨터 시스템의 전체 또는 일부에 대한 권한 없는 액세스
2. 불법적인 가로채기: 권한 없이 기술적인 수단에 의한 가로채기 또는 컴퓨터 시스템 내외부로 또는 컴퓨터 시스템 내에서의 컴퓨터 데이터 비공개 전송 가로채기(여기에는 그러한 컴퓨터 데이터를 전달하는 컴퓨터 시스템의 전자기 방사가 포함됨)
3. 데이터 간섭: 권한 없이 컴퓨터 데이터에 대한 손상, 삭제, 악화, 변경, 억제 또는 액세스 거부
4. 시스템 간섭: 권한 없이 컴퓨터 데이터를 입력, 전송, 손상, 삭제, 악화, 변경 또는 억제하여 컴퓨터 시스템의 기능을 심각하게 방해
5. 장치의 오용: (a) 주로 위에 열거한 위법 행위를 저지르기 위한 목적으로 설계하거나 개조한 컴퓨터 프로그램 또는 컴퓨터 코드가 포함된 장치 또는 (b) 위에 열거한 위법 행위를 저지르기 위한 목적에 사용할 의도로 컴퓨터 시스템의 전체 또는 일부에 액세스하는 데 사용할 수 있는 컴퓨터 암호, 액세스 코드, 자격 증명 또는 이와 유사한 데이터의 생산, 판매, 사용을 위한 조달, 수입 또는 유통이나 다른 방법으로 사용할 수 있게 만드는 것"

사이버 보안 사고. 사이버 보안 사고는 "정보 보안 정책에 대해 일어날 수 있는 위반 또는 보안 컨트롤의 실패를 나타내는 것으로 시스템, 서비스 또는 네트워크에 대해 확인된 단일 또는 일련의 사건이거나 시스템, 서비스 또는 네트워크의 보안과 관련된 이전에 알려지지 않은 상황" 으로 정의할 수 있습니다.

사이버 보안 서비스. 사이버 보안 서비스는 "주로 사이버 보안 위협을 탐지, 완화 또는 방지하기 위해 설계된 제품, 상품 또는 서비스"로 정의할 수 있습니다.

사이버 보안 위협. 사이버 보안 위협은 "정보 시스템에 저장되거나 정보 시스템에 의해 처리되거나 정보 시스템을 통과하는 정보 또는 정보 시스템에 대한 무단 액세스, 변조, 조작 또는 손상, 이러한 정보 또는 정보 시스템의 무결성, 기밀성 또는 가용성에 대한 손상을 초래할 수 있는 모든 행위"로 정의할 수 있습니다.

사이버 보안 위협 지표. 사이버 보안 위협 지표는 다음과 같이 정의할 수 있습니다.

"다음을 설명하거나 확인하는 데 필요한 정보

1. 사이버 보안 위협 또는 보안 취약성과 관련된 기술 정보를 수집하기 위한 목적으로 전송되는 것처럼 보이는 비정상적인 통신 패턴이 포함된 악의적인 정찰
2. 보안 컨트롤을 무력화하거나 보안 취약성을 악용하는 방법
3. 보안 취약성이 있음을 나타내는 것처럼 보이는 비정상적인 활동을 비롯한 보안 취약성
4. 정보 시스템에 저장되거나 정보 시스템에 의해 처리되거나 정보 시스템을 통과하는 정보 또는 정보 시스템에 대한 합법적인 액세스 권한을 가진 사용자가 자신도 모르게 보안 컨트롤을 무력화하거나 보안 취약성을 악용할 수 있게 만드는 방법
5. 악의적인 사이버 명령 및 통제
6. 특정한 사이버 보안 위협의 결과로 노출된 정보에 대한 설명을 비롯하여 사고로 인한 실제 또는 잠재적 피해

7. 사이버 보안 위협의 기타 특성(그러한 특성의 공개가 달리 법으로 금지되지 않은 경우) 또는

8. 앞에 언급된 항목들의 조합"

방어 조치. 방어 조치는 "알려져 있거나 의심되는 사이버 보안 위협 또는 보안 취약성을 탐지, 방지 또는 완화하기 위해 정보 시스템에 저장되거나 정보 시스템에 의해 처리되거나 정보 시스템을 통과하는 정보 또는 정보 시스템에 적용하는 동작, 장치, 절차, 서명, 기술 또는 기타 조치"로 정의할 수 있습니다.

정보 보안. 정보 보안은 다음과 같이 정의할 수 있습니다.

"정보 및 정보 시스템이 무단 액세스, 사용, 공개, 중단, 수정 또는 파괴되지 않도록 보호하여 다음을 제공합니다.

1. 무결성 - 부적절한 정보 수정 또는 파괴로부터 보호하는 것을 의미하며, 부인 방지 및 진본성 보장이 포함됩니다.

2. 기밀성 - 액세스 및 공개에 대해 허가된 제한을 유지하는 것을 의미하며, 개인 사생활 및 독점 정보를 보호하기 위한 수단이 포함됩니다.

3. 가용성 - 정보에 대한 시기적절하고 신뢰할 수 있는 액세스 및 사용을 보장하는 것을 의미합니다."

정보 시스템. 정보 시스템은 "정보의 수집, 처리, 유지, 사용, 공유, 배포 또는 폐기를 위해 조직된 정보 리소스의 개별 세트"로 정의할 수 있습니다.

국제적으로 인정받은 표준. 표준은 "국제적인 합의에 의해 제정되고 인정된 조직에 의해 승인되며 광범위하게 채택된 문서로, 공통적이고 반복적인 사용을 위해 정해진 맥락에서 최적의 수준 달성을 목표로 하는 활동 또는 그 결과에 대한 규칙, 지침 또는 특성을 규정한 것으로 정의할 수 있습니다. 표준은 소비자를 포함하여 모든 국제 이해 관계자에게 자신의 견해를 표현하고 해당 견해를 고려할 수 있는 기회를 제공하는 열린 프로세스 내에서 개발된 자발적 협약입니다. 이는 공정성 및 시장 적합성에 기여하고 사용 시 신뢰를 증진시킵니다."

위험. 위험은 "제품 또는 시스템에 대해 확인된 위협 분석, 해당 제품 또는 시스템의 알려진 취약성 그리고 제품 또는 시스템 손상의 잠재적 결과를 통해 파악할 수 있는, 완벽한 보안이라는 사이버 보안 목표에서 불확실성의 결과가 표출된 것"으로 정의할 수 있습니다.

보안 컨트롤. 보안 컨트롤은 "정보 시스템 또는 해당 정보의 기밀성, 무결성 및 가용성에 악영향을 미칠 수 있는 권한 없는 활동으로부터 보호하는 데 사용되는 관리, 운영 또는 기술 제어"로 정의할 수 있습니다.

중요한 사이버 보안 사고. 중요한 사이버 보안 사고는 "다음과 같은 결과를 초래하는 사이버 보안 사고"로 정의할 수 있습니다."

- 중요 인프라 운영에 필수적인 데이터에 대한 손상, 삭제, 변경, 억제 또는 무단 액세스나 액세스 거부 또는
- 중요 인프라의 보안 또는 운영에 필수적인 운영 제어 또는 기술 제어의 무력화

BSA 소개

BSA | The Software Alliance(www.bsa.org)는 각국의 정부 및 국제 시장을 상대로 글로벌 소프트웨어 업계의 목소리를 대변하는 선두 단체입니다. 회원사들은 경제 진흥을 지원하고 현대의 삶을 향상시키는 소프트웨어 솔루션을 만드는 세계에서 가장 혁신적인 회사들입니다.

워싱턴 DC에 본부를 두고 60여 개국에 지부를 두고 있는 BSA는 합법적인 소프트웨어 사용을 장려하고 기술 혁신 활성화 및 디지털 경제 성장을 위한 공공 정책을 지지하는 컴플라이언스 프로그램을 주도합니다.



www.bsa.org

BSA 세계 본부

20 F Street, NW
Suite 800
Washington, DC 20001

+1.202.872.5500
@BSAnews
@BSATheSoftwareAlliance

BSA 아시아 태평양

300 Beach Road
#25-08 The Concourse
Singapore 199555

+65.6292.2072
@BSAnewsAPAC

BSA 유럽, 중동 및 아프리카

65 Petty France
Ground Floor
London, SW1H 9EU
United Kingdom

+44.207.340.6080
@BSAnewsEU